Principaux avantages

Prévention

- Identifier les failles de sécurité dans l'ensemble de l'environnement pour hiérarchiser les correctifs
- Détecter les contrôles de sécurité mal configurés ou défectueux qui pourraient être exploités
- Inspecter attentivement les accès à haut risque vers des ressources ou des données précieuses à l'aide de tests d'infiltration annuels
- Améliorer la vigilance des collaborateurs grâce à des formations sur la sécurité dispensées sous forme de modules courts et réguliers

Réponse

- Détecter les menaces dans l'environnement et y répondre 24x7
- Suivre l'activité des pirates de bout en bout
- Utiliser la télémétrie et corréler les événements de nombreux outils de sécurité populaires

Dell Managed Detection and Response Pro Plus

Solution SecOps complète entièrement gérée pour les points de terminaison, le réseau et le Cloud

Relever les défis stratégiques liés aux opérations de sécurité

De nombreux départements IT ont adopté la surveillance et la détection des menaces pour faire face à l'augmentation constante du volume et de la variété des menaces.

Bien que la surveillance et la détection des menaces fournissent une couverture indispensable, il est préférable de colmater les brèches dès le départ, avant que les pirates n'aient l'occasion de les exploiter. Les équipes IT peuvent bloquer une grande partie des activités malveillantes en traitant proactivement les failles de sécurité des logiciels, les contrôles de sécurité mal configurés et l'imprudence des collaborateurs.

Des professionnels de la sécurité compétents savent corriger les failles de sécurité, toutefois, la majorité des départements IT n'ont pas les moyens de les corriger toutes. En 2021, plus de 1 500 nouvelles failles de sécurité ont été signalées chaque mois[1]. Pour que la charge des correctifs reste gérable, les clients doivent hiérarchiser les failles de sécurité présentant le plus de risques.

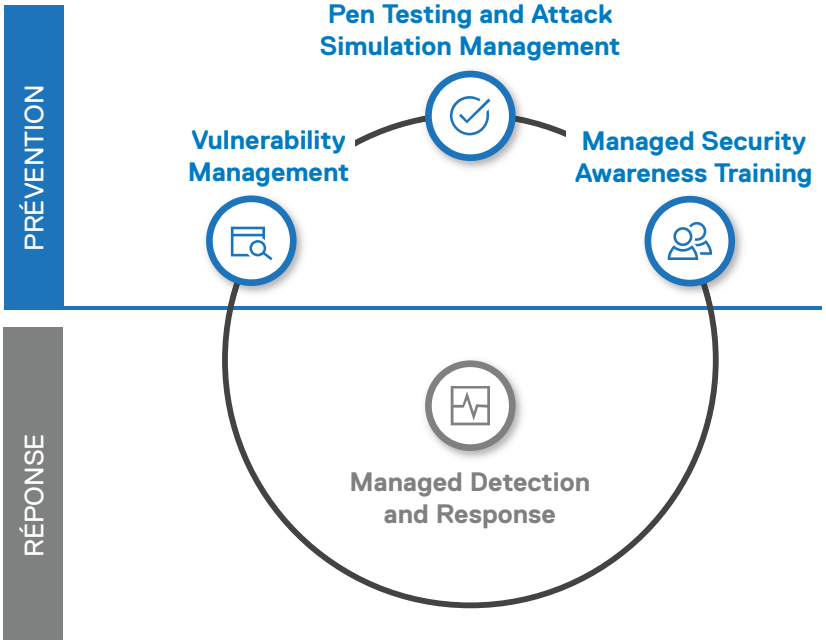
Il est tout aussi complexe d'essayer de valider tous vos contrôles de sécurité, tels que les passerelles de messagerie ou les pare-feu d'applications Web. Avec des centaines de contrôles et de configurations complexes, les équipes de sécurité IT ont du mal à vérifier si les contrôles de sécurité bloquent bien les activités non autorisées.

En outre, les organisations ont besoin que les collaborateurs sachent reconnaître quand les pirates tentent d'obtenir leurs informations d'identification, des données confidentielles ou d'autres données sensibles. Une étude a révélé que 83 % des organisations interrogées ont été victimes d'une attaque par phishing réussie en 2021[2].

Managed Detection and Response Pro Plus

Les experts en sécurité Dell Technologies ont examiné de près ces préoccupations SecOps clés afin de concevoir un nouveau service d'opérations de sécurité complet°: Managed Detection and Response Pro Plus.

MDR Pro Plus est une solution SecOps entièrement gérée via laquelle les meilleurs experts du domaine de la sécurité utilisent des outils de pointe pour prévenir les menaces, détecter et contenir rapidement les tentatives d'attaque, puis lancer un processus de récupération en cas de violation. MDR Pro Plus vous aide à renforcer continuellement la posture de sécurité de votre organisation.



Colmater les brèches des logiciels et contrôles de sécurité

Le service **Vulnerability Management** analyse votre environnement tous les mois pour rechercher les failles de sécurité et utilise l'apprentissage automatique pour donner la priorité à celles les plus susceptibles d'être exploitées et d'avoir un impact majeur sur l'entreprise. La liste hiérarchisée permet à votre équipe IT de se concentrer sur les plus importantes failles de sécurité.

Comme les pirates savent trouver les failles de sécurité non corrigées et les contrôles de sécurité mal configurés ou obsolètes, les départements IT doivent les trouver et les corriger en priorité. Le service **Pen Testing and Attack Simulation Management** offre des simulations mensuelles automatisées Breach and Attack Simulation (BAS) et des tests d'infiltration annuels.

BAS détecte les contrôles de sécurité défectueux sur les appareils et les logiciels de votre environnement IT. Les tests d'infiltration viennent compléter le service BAS en essayant d'atteindre un objectif spécifique, comme un système à forte valeur ajoutée. Les testeurs d'infiltration qualifiés reproduisent les techniques des pirates, en modifiant et en adaptant les techniques pour atteindre la cible.

Dell exécute des analyses de failles de sécurité et des simulations BAS sur des bases de données continuellement mises à jour pour vous aider à vous assurer que les correctifs et les contrôles de sécurité restent à jour.

Aider les collaborateurs à rester vigilants

Un modèle commun de formation de sensibilisation à la sécurité est une session de formation annuelle de plusieurs heures. Toutefois, il arrive souvent que les collaborateurs ne retiennent pas ces informations, qui peuvent simplement devenir des « cases à cocher ». S'ils sont confrontés à une tactique d'ingénierie sociale ou à un e-mail contenant un lien malveillant, ils risquent de manquer de vigilance.

Managed Security Awareness Training propose de courtes formations de sécurité tout au long de l'année, ce qui permet aux collaborateurs de s'engager activement dans des cursus personnalisés et de faire de la sécurité une priorité. Les cursus sont créés en fonction du rôle des collaborateurs, du niveau d'exposition aux menaces et de la progression.

Détecter et contenir rapidement les tentatives d'attaque

Dell MDR Pro Plus offre une **détection et une réponse gérées** 24x7. Des analystes qualifiés surveillent votre environnement et étudient les menaces à l'aide d'une plateforme d'analytique de sécurité XDR avancée. Les analyses basées sur l'apprentissage automatique et le Deep Learning de la télémétrie et des événements fournissent aux analystes de nombreuses informations pour reconstituer le parcours et les activités du pirate. L'équipe Dell vous fournit ensuite des instructions pour vous aider à contenir et corriger le problème. En cas d'incident de sécurité, Dell Technologies vous aide à lancer le processus de sauvegarde et d'exécution de votre organisation.

Optimiser les opérations de sécurité avec Dell

MDR Pro Plus aide à prévenir les activités malveillantes en vous informant régulièrement des failles de sécurité, des contrôles de sécurité mal configurés et des accès à haut risque vers des ressources précieuses. En outre, nous proposons des formations concises et pratiques sur la sécurité pour les collaborateurs tout au long de l'année. La détection et la réponse aux menaces assurent une surveillance et un suivi en permanence des activités suspectes.

MDR Pro Plus vous fournit une solution intelligente pour les opérations de sécurité IT, avec des services basés sur une technologie avancée, fournis par des experts. Le tout géré par Dell Technologies : une société à laquelle les organisations de toutes tailles du monde entier font confiance en matière d'appareils, d'infrastructures et de services IT innovants.

Pour en savoir plus sur Dell Managed Detection and Response Pro Plus

Contacter un expert Dell Technologies

[1] Source : With 18,378 vulnerabilities reported in 2021, NIST records fifth straight year of record numbers, ZDNet, 8 décembre 2021. https://www.zdnet.com/article/with-18376-vulnerabilities-found-in-2021-nist-reports-fifth-straight-year-of-record-numbers/

[2] Source : 2020 Phishing Attack Landscape Report [Greathorn]. Cybersecurity Insiders. (2020). Consulté le 15 novembre 2022 sur https://www.cybersecurity-insiders.com/portfolio/2020-phishing-attack-landscape-report-greathorn/